CLAIMS

1. An application server embodied in a computer, comprising:

a user list, including a user name and a cleartext password associated with the user name;

an authenticator to authenticate the cleartext password using an authentication server;

a hasher to hash the cleartext password to produce a hashed password;

a comparator to compare the hashed password with a received hashed password; and

a client services provider to receive the received hashed password from a workstation and to transmit a result from the comparator to the workstation.

2. An application server according to claim 1, wherein the hasher includes a hashing algorithm associated with the workstation.

3. An application server according to claim 2, wherein the hasher includes a second hashing algorithm associated with a second workstation.

4. An application server according to claim 2, wherein hasher includes a second hashing algorithm associated with the workstation.

5. An application server according to claim 1, wherein the client services provider is operative to receive the cleartext password from the workstation.

6. An application server according to claim 1, wherein:

the client services provider is operative to receive a new cleartext password from the workstation; and

the application server further comprises a replacer to replace the cleartext password with the new cleartext password.

7. A system, comprising:

a network;

a workstation coupled to the network, the workstation including:

a first user name and a first cleartext password; and

a first hasher to hash the first cleartext password to produce a first hashed password;

an authentication server coupled to the network, the authentication server including a second user name and a second cleartext password associated with the second user name; and

an application server coupled to the network, the application server including:

a user list including a third user name and a third cleartext password associated with the third user name;

an authenticator to authenticate the third cleartext password to the second cleartext password using the authentication server;

a second hasher to hash the third cleartext password to produce a second hashed password;

a comparator to compare the first hashed password with the second hashed password; and

a client services provider to receive the received hashed password from a workstation and to transmit a result from the comparator to the workstation.

8. A system according to claim 7, wherein:

the first hasher includes a first hashing algorithm; and

the second hasher includes the first hashing algorithm, the first hashing algorithm associated with the workstation.

9. A system according to claim 8, wherein the second hasher includes a second hashing algorithm associated with a second workstation.

10. A system according to claim 7, wherein:

the receiver is operative to receive a new cleartext password from the workstation; and

the application server further comprises a replacer to replace the cleartext password with the new cleartext password.

11. A system according to claim 10, wherein the transmitter is operative to forward the new cleartext password to the authentication server.

12. A method for authenticating a user on an application server, comprising:

receiving a user name and a hashed password from a first workstation;

determining a cleartext password associated with the user name;

authenticating the cleartext password to a second password using an authentication server;

determining a hashing algorithm used by the first workstation;

hashing the cleartext password using the hashing algorithm to produce a computed hashed password;

comparing the received hashed password with the computed hashed password; and

if the received hashed password matches the computed hashed password, authenticating the user.

13. A method according to claim 12, further comprising, if the received hashed password does not match the computed hashed password, failing to authenticating the user.

14. A method according to claim 12, further comprising selecting the authentication server from a plurality of authentication servers.

15. A method according to claim 12, wherein authenticating the cleartext password to a second password includes binding the cleartext password to the second password on the authentication server using a Lightweight Directory Access Protocol (LDAP).

16. A method according to claim 12, wherein determining a hashing algorithm used includes selecting the hashing algorithm from a plurality of hashing algorithms.

17. A method according to claim 16, further comprising adding a new hashing algorithm to the plurality of hashing algorithms.

18. A method according to claim 17, wherein adding a new hashing algorithm includes associating the hashing algorithm with at least one of a set of workstations, the set of workstations including the first workstation.

19. A method according to claim 12, wherein determining a cleartext password includes:

determining that the cleartext password does not exist on the application server;

requesting from the user the cleartext password; and

receiving from the user the cleartext password.

20. A method according to claim 12, further comprising:

receiving a request from the workstation to change the cleartext password to a new cleartext password; and

replacing the cleartext password with the new cleartext password.

21. A method according to claim 20, further comprising forwarding the new cleartext password to the authentication server.

22. An article comprising a machine-accessible medium having associated data, wherein the data, when accessed, results in a machine performing:

receiving a user name and a hashed password from a first workstation;

determining a cleartext password associated with the user name;

authenticating the cleartext password to a second password using an authentication server;

determining a hashing algorithm used by the first workstation;

hashing the cleartext password using the hashing algorithm to produce a computed hashed password;

comparing the received hashed password with the computed hashed password; and

if the received hashed password matches the computed hashed password, authenticating the user.

23. An article according to claim 22, the machine-accessible data further including associated data that, when accessed, results in, if the received hashed password does not match the computed hashed password, failing to authenticating the user.

24. An article according to claim 22, the machine-accessible data further including associated data that, when accessed, results in selecting the authentication server from a plurality of authentication servers.

25. An article according to claim 22, wherein authenticating the cleartext password to a second password includes binding the cleartext password to the second password on the authentication server using a Lightweight Directory Access Protocol (LDAP).

26. An article according to claim 22, wherein determining a hashing algorithm used includes selecting the hashing algorithm from a plurality of hashing algorithms.

27. An article according to claim 26, the machine-accessible data further including associated data that, when accessed, results in adding a new hashing algorithm to the plurality of hashing algorithms.

28. An article according to claim 27, wherein adding a new hashing algorithm includes associating the hashing algorithm with at least one of a set of workstations, the set of workstations including the first workstation.

29. An article according to claim 22, wherein determining a cleartext password includes:

determining that the cleartext password does not exist on the application server;

requesting from the user the cleartext password; and

receiving from the user the cleartext password.

30. An article according to claim 22, the machine-accessible data further including associated data that, when accessed, results in:

receiving a request from the workstation to change the cleartext password to a new cleartext password; and

replacing the cleartext password with the new cleartext password.

31. An article according to claim 30, the machine-accessible data further including associated data that, when accessed, results in forwarding the new cleartext password to the authentication server.